TITLE:

2元2次不定方程式の整数解のOSTROWSKI表現について (代数的整数論とその周辺)

AUTHOR(S):

橋本, 竜太

CITATION:

橋本, 竜太. 2元2次不定方程式の整数解のOSTROWSKI表現について (代数的整数論とその周辺). 数理解析研究所講究録 2000, 1154: 155-164

ISSUE DATE:

2000-05

URL:

http://hdl.handle.net/2433/64118

RIGHT:

京都大学学術情報リポジトリ
KURENAI 紅
Kyoto University Research Information Repository

数理解析研究所講究録
1154巻 2000年 155-164

2元2次不定方程式の整数解のOSTROWSKI表現について

橋本竜太 (HASHIMOTO, RYŪTA)
（名古屋大学大学院人間情報学研究科ＤＣ）

ABSTRACT. 整数のOstrowski表現なる概念を導入することで, $x^2 - Dy^2 = N$ の整数解が, ある種の形で一意的に表されることがわかる. さらに, より一般的に, $Ax^2 + Bxy + Cy^2 = N$ の整数解に関しても同様のことが成り立つことも確認される.

1. 正整数のOSTROWSKI表現

実数 α に対して, 整数列 $\{a_k\}_{k\geq 0}$ および実数列 $\{\alpha_k\}_{k\geq 0}$ を

$$\alpha_0 = \alpha, \quad a_k = \lfloor \alpha_k \rfloor, \quad \alpha_{k+1} = \frac{1}{\alpha_k - a_k} \tag{1}$$

で定義すると, α の連分数展開

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}} =: [a_0, a_1, a_2, \ldots]$$

が得られる. 整数列 $\{p_k\}_{k\geq -1}$, $\{q_k\}_{k\geq -1}$ を次で定める:

$$p_{-1} = 1, \quad p_0 = a_0, \quad p_k = a_k p_{k-1} + p_{k-2} \quad (k \geq 1); \tag{2}$$

$$q_{-1} = 0, \quad q_0 = 1, \quad q_k = a_k q_{k-1} + q_{k-2} \quad (k \geq 1). \tag{3}$$

このとき, 次のことが成り立つことはよく知られている:

$$\frac{p_k}{q_k} = [a_0, \ldots, a_k], \quad \lim_{k\to\infty} \frac{p_k}{q_k} = \alpha.$$

さて, y を正整数とする. $\{q_k\}$ は $q_1 = 1$ である場合の $q_0 = q_1$ を除いて狭義単調増加であるので, $q_n \leq y < q_{n+1}$ なる n が一意に決まる. そして, $y = c_{n+1}q_n + y'$ かつ $0 \leq y' < q_n$ なる整数 c_{n+1}, y' も一意に決

Date: 2000(平成12)年1月27日, 研究集会「代数的整数論とその周辺」(京大数理研).

まる. $y' \neq 0$ であれば, $q_{n'} \leq y < q_{n'+1}$ なる n' が一意に決まり, さらに, $y' = c_{n'+1}q_{n'} + y''$ かつ $0 \leq y'' < q_{n'}$ なる整数 $c_{n'+1}$, y'' も一意に決まる. この操作を繰り返すと, $q_0 = 1$ なるがゆえに, 必ず操作は停止する. そして, $\{q_n\}$ の線型和としての y の表現が得られる:

$$y = c_1q_0 + c_2q_1 + \cdots + c_{n+1}q_n.$$

ここで, $\{c_k\}$ は次を満たしていることがわかる:

- $0 \leq c_k \leq a_k$ $(k > 1)$, $0 \leq c_1 < a_1$;
- $c_k = a_k$ ならば $c_{k-1} = 0$.

逆に, 正整数を $\{q_k\}$ の線型和で表すとき, 係数 $\{c_k\}$ に上記の条件を満たすことを要請すれば, その線型和の表現は一意に定まることがわかる. これを, 正整数の α に関する Ostrowski 表現と呼ぶことにしよう.

2. 正整数の平方根の連分数展開

D は平方数ではない正整数とする. $\sqrt{D}$ の連分数展開は

$$\sqrt{D} = [a_0, \overline{a_1, a_2, \ldots, a_{l-1}, 2a_0}]$$

と表されることが知られている. すなわち, $\{a_k\}$ に関して次が成り立つ:

$$a_{k+l} = a_k \quad (k \geq 1), \quad a_l = 2a_0.$$

なお, 以下では l は上の式を満たす最小の正整数とし, この l を連分数展開の周期の長さとよぶこととする.

例 1. $\sqrt{34}$ の連分数展開は次の通り. なお, 周期の長さは 4.

$$\sqrt{34} = [5, \overline{1, 4, 1, 10}]$$

k	-1	0	1	2	3	4	5	6
a_k		5	1	4	1	10	1	4
p_k	1	5	6	29	35	379	414	2035
q_k	0	1	1	5	6	65	71	349

k	7	8	9	10	11
a_k	1	10	1	4	1
p_k	2449	26525	28974	142421	171395
q_k	420	4549	4969	24425	29394

□

3. ROCKETT-SZÜSZ の定理

整数の Ostrowski 表現に関連して, 次の定理が成り立つ:

定理 1 (Rockett and Szüsz [4], [5], 橋本 [2]). D は平方数ではない正整数, N は 0 ではない整数とする. $\alpha = \sqrt{D}$ として, 整数列 $\{a_k\}_{k\geq 0}$, $\{p_k\}_{k\geq -1}$, $\{q_k\}_{k\geq -1}$ を (1), (2), (3) で定義する. また, $\epsilon = \min\bigl(\sqrt{D} - a_0, 1/(2\sqrt{2}), (1 + a_0 - \sqrt{D})/\sqrt{2}\bigr)$ とする.

(x, y) は $x^2 - Dy^2 = N$ の正整数解であるとする. y が十分大きければ, すなわち, $y > |N|/(2\epsilon\sqrt{D})$ ならば, x, y は次のような形で一意的に表される:

$$x = c_{n+1}p_n + c_{n+2}p_{n+1} + \cdots + c_{n+m}p_{n+m-1},$$

$$y = c_{n+1}q_n + c_{n+2}q_{n+1} + \cdots + c_{n+m}q_{n+m-1}.$$

ただし, $\{c_k\}$ は次を満たすものとする:

1. $c_{n+1} \neq 0$, $c_{n+m} \neq 0$;
2. $0 \leq c_{n+k} \leq a_{n+k}$ $(n + k \neq 1)$, $0 \leq c_1 < a_1$;
3. $c_{n+k} = a_{n+k}$ ならば $c_{n+k-1} = 0$.

さらに, $N > 0$ ならば n は奇数, $N < 0$ ならば n は偶数である. そして, 線型和の長さ m の範囲は D と N により次のように評価できる:

$$(4)\quad \frac{1}{\log(1 + a_0) + (\log 2)/l} \cdot \log \frac{|N|}{4\sqrt{D}} < m < \max\left(3, 3 + \log_\tau \sqrt{5} + \log_\tau \frac{|N|}{\sqrt{D}}\right).$$

ただし, $\tau = (1 + \sqrt{5})/2$. □

平たくいうならば, y の $\sqrt{D}$ に関する Ostrowski 表現において q を p に換えたものが x に等しいということである. ただし, y が十分大きくないときにはそうはいかないこともある. [4, Theorem 2], [5, Theorem IV.2.3] ではその点に関する議論が欠落している.

例 2. $(5417, 929)$ は $x^2 - 34y^2 = 495$ の整数解. 929 の $\sqrt{34}$ に関する Ostrowski 表現は $929 = 3q_3 + q_5 + 2q_7$. 一方, $3p_3 + p_5 + 2p_7 = 5417$. □

例 3. $(79, 13)$ も $x^2 - 34y^2 = 495$ の整数解. 13 の $\sqrt{34}$ に関する Ostrowski 表現は $13 = q_1 + 2q_3$. ところが, $p_1 + 2p_3 = 76 \neq 79$. □

4. 整数解の周期性

$\sqrt{D}$ の連分数展開の周期性に関連して, 2 元 2 次不定方程式の整数解にもある種の周期性が見られることがわかる.

定理 2. D は平方数ではない正整数, N は 0 ではない整数とする. $\alpha = \sqrt{D}$ として, 整数列 $\{a_k\}_{k\geq 0}$, $\{p_k\}_{k\geq -1}$, $\{q_k\}_{k\geq -1}$ を (1), (2), (3) で定義する. また, l を $\sqrt{D}$ の連分数展開の周期の長さとする.

整数列 $\{c_k\}$ が与えられたとき, 次の条件は同値である:

1. 次の (x, y) は $x^2 - Dy^2 = N$ の整数解である:

$$x = c_{n+1}p_n + c_{n+2}p_{n+1} + \cdots + c_{n+m}p_{n+m-1},$$

$$y = c_{n+1}q_n + c_{n+2}q_{n+1} + \cdots + c_{n+m}q_{n+m-1}.$$

2. 次の (x, y) は $x^2 - Dy^2 = (-1)^l N$ の整数解である:

$$x = c_{n+1}p_{n+l} + c_{n+2}p_{n+1+l} + \cdots + c_{n+m}p_{n+m-1+l},$$

$$y = c_{n+1}q_{n+l} + c_{n+2}q_{n+1+l} + \cdots + c_{n+m}q_{n+m-1+l}.$$

□

この定理は, たとえば次の補題を利用して証明できる:

補題 1. $\{p_k\}_{k\geq -1}$, $\{q_k\}_{k\geq -1}$, l は定理 2 におけるものとするとき, $k \geq -1$ に対して, 次が成り立つ:

$$\begin{pmatrix} p_{k+l} \\ q_{k+l} \end{pmatrix} = \begin{pmatrix} p_{l-1} & Dq_{l-1} \\ q_{l-1} & p_{l-1} \end{pmatrix} \begin{pmatrix} p_k \\ q_k \end{pmatrix} \tag{5}$$

□

例 4. $(5417, 929)$ は $x^2 - 34y^2 = 495$ の整数解であり,

$$5417 = 3p_3 + p_5 + 2p_7, \quad 929 = 3q_3 + q_5 + 2q_7$$

であった.

添字を $l = 4$ ずつ増やしてみると,

$$3p_7 + p_9 + 2p_{11} = 379111, \quad 3q_7 + q_9 + 2q_{11} = 65017.$$

そして, $(379111, 65017)$ が $x^2 - 34y^2 = 495$ の解であることは直接の計算でも確認できる.

今度は添字を 4 ずつ減らしてみると,

$$3p_{-1} + p_1 + 2p_3 = 79, \quad 3q_{-1} + q_1 + 2q_3 = 13.$$

先の例にあるように, $(79, 13)$ は $x^2 - 34y^2 = 495$ の解. □

補題 1 を逆手にとって, $\{p_k\}_{k<-1}$, $\{q_k\}_{k<-1}$ を (5) で帰納的に定義してしまおう. すると, 次の定理が成り立つことは容易にわかる:

定理 3. $\{p_k\}_{k\in\mathbb{Z}}$, $\{q_k\}_{k\in\mathbb{Z}}$ を (2), (3), (5) で定義する. このとき, 定理 2 は任意の整数 n について成り立つ. □

例 5. $\sqrt{34}$ の連分数展開において, $\{p_k, q_k\}_{k=-3,-5}$ を次で定義する:

$$\begin{pmatrix} p_{-3} \\ q_{-3} \end{pmatrix} := \begin{pmatrix} p_3 & 34q_3 \\ q_3 & p_3 \end{pmatrix}^{-1} \begin{pmatrix} p_1 \\ q_1 \end{pmatrix} = \begin{pmatrix} 6 \\ -1 \end{pmatrix},$$

$$\begin{pmatrix} p_{-5} \\ q_{-5} \end{pmatrix} := \begin{pmatrix} p_3 & 34q_3 \\ q_3 & p_3 \end{pmatrix}^{-1} \begin{pmatrix} p_{-1} \\ q_{-1} \end{pmatrix} = \begin{pmatrix} 35 \\ -6 \end{pmatrix}.$$

すると,

$$3p_{-5} + p_{-3} + 2p_{-1} = 113, \quad 3q_{-5} + q_{-3} + 2q_{-1} = -19.$$

そして, $(113, -19)$ が $x^2 - 34y^2 = 495$ の解であることは直接の計算で確認できる. □

さらに, $\{a_k\}_{k\leq -1}$ を次で定義しよう:

$$a_k = a_{k+jl} \quad (j \gg 0). \tag{6}$$

すると, 次のことが確認される:

補題 2. (1), (2), (3), (5), (6) で定義された $\{a_k\}_{k\in\mathbb{Z}}$, $\{p_k\}_{k\in\mathbb{Z}}$, $\{q_k\}_{k\in\mathbb{Z}}$ について, 次が成り立つ:

$$p_k = a_k p_{k-1} + p_{k-2}, \qquad q_k = a_k q_{k-1} + q_{k-2} \quad (k \neq 0),$$
$$p_0 = 2a_0 p_{-1} + p_{-2}, \qquad q_0 = 2a_0 q_{-1} + q_{-2}.$$

□

例 6. $\sqrt{34}$ の連分数展開における $\{a_k\}$, $\{p_k\}$, $\{q_k\}$.

k	-1	-2	-3	-4	-5	-6	-7	-8	-9
a_k	1	4	1	10	1	4	1	10	1
p_k	1	-5	6	-29	35	-379	414	-2035	2449
q_k	0	1	-1	5	-6	65	-71	349	-420

□

5. 整数解の OSTROWSKI 表現

前節の考察は, $\{p_k\}_{k\in\mathbb{Z}}$, $\{q_k\}_{k\in\mathbb{Z}}$ をうまく定義すれば, 定理 1 において「y が十分大きければ」という仮定を除くことができることを示唆している。実際, $\{a_k\}_{k\in\mathbb{Z}}$, $\{p_k\}_{k\in\mathbb{Z}}$, $\{q_k\}_{k\in\mathbb{Z}}$ を (1), (2), (3), (6), および補題 1 (または補題 2) により定義すれば, 次の定理が成り立つ.

定理 4. (x, y) は $x^2 - Dy^2 = N$ の整数解であるとする. ここで, $N > 0$ ならば $x > 0$, $N < 0$ ならば $y > 0$ とする. さもなくば, $(-x, -y)$ を改めて (x, y) にとる.

このとき, x, y は次の形で一意的に表される:

$$x = c_{n+1}p_n + c_{n+2}p_{n+1} + \cdots + c_{n+m}p_{n+m-1},$$
$$y = c_{n+1}q_n + c_{n+2}q_{n+1} + \cdots + c_{n+m}q_{n+m-1}.$$

ただし, $\{c_k\}$ は次を満たすものとする:

1. $c_{n+1} \neq 0$, $c_{n+m} \neq 0$;

2. $0 \leq c_{n+k} \leq a_{n+k}$ $(n+k \neq 0)$, $0 \leq c_0 \leq 2a_0$;
3. $n+k \neq 0$ かつ $c_{n+k} = a_{n+k}$ ならば $c_{n+k-1} = 0$.
   また, $c_0 = 2a_0$ ならば $c_{-1} = 0$.

さらに, 線型和の長さ m の範囲は (4) で評価できる. □

ところで, 定理 4 に至っては, たとえ $y > 0$ であっても, その形は 1 節にいう Ostrowski 表現であるとは限らない. しかしながら, x と y の組として考えると表現は一意的であり, その一意性は整数の Ostrowski 表現の一意性より導かれる. そこで, 定理 4 における整数解の形を, 不定方程式 $x^2 - Dy^2 = N$ に関する Ostrowski 表現と呼んでもよいであろう.

なお, 定理 4 に基づいて $x^2 - Dy^2 = N$ の整数解を求めるプログラムを PARI-GP 上に実現したものを [1] として公開している. ただし, 実行速度は速いとはいえない.

6. より一般的な場合

$Ax^2 + Bxy + Cy^2 = N$ の整数解について考えよう. ただし, A, B, C, N は整数で, $A > 0$, $\gcd(A, B, C) = 1$, $N \neq 0$ であるものとし, $D := B^2 - 4AC$ は平方数ではない正整数であるとする. $\alpha = (-B + \sqrt{D})/(2A)$ としよう. α は $Ax^2 + Bx + C$ の根であることに注意しておく.

$\{a_k\}_{k \geq 0}$ を (1) で定義すると, α の連分数展開

$$\alpha = [a_0, a_1, \ldots, a_{s-1}, \overline{a_s, a_{s+1}, \ldots, a_{s+l-1}}]$$

が得られる. すなわち, $\{a_k\}$ について次が成り立つ:

$$a_{k+l} = a_k \quad (k \geq s). \tag{7}$$

なお, 以下では l, s は $l > 0$, $s \geq 0$, かつ (7) を満たす正整数のうち最小のものとする. そして, l を α の連分数展開の周期の長さ, s を前周期の長さと呼ぶことにしよう.

$\{p_k\}$, $\{q_k\}$ を (2), (3) で定義する. さらに, $\{a'_k\}_{k \in \mathbb{Z}}$, $\{p'_k\}_{k \in \mathbb{Z}}$, $\{q'_k\}_{k \in \mathbb{Z}}$ を次で定義する:

$$a'_k = \begin{cases} a_k & (k \geq s), \\ a_{k+jl} \quad (j \gg 0) & (k < s), \end{cases}$$

$$p'_k = \begin{cases} p_k & (k \geq s-2), \\ p'_{k+2} - a'_{k+2}p'_{k+1} & (k < s-2), \end{cases}$$

$$q'_k = \begin{cases} q_k & (k \geq s-2), \\ q'_{k+2} - a'_{k+2}q'_{k+1} & (k \leq s-2). \end{cases}$$

以上の準備の元で, 補題1, 定理3および定理4の拡張として次のことが成り立つことが確認できる:

補題 3. $k \in \mathbb{Z}$ に対して, 次が成り立つ:

$$\begin{pmatrix} p'_{k+l} \\ q'_{k+l} \end{pmatrix} = \left\{ (-1)^{s-1} \begin{pmatrix} p_{s+l} & p_{s+l-1} \\ q_{s+l} & q_{s+l-1} \end{pmatrix} \begin{pmatrix} q_{s-1} & -p_{s-1} \\ -q_s & p_s \end{pmatrix} \right\} \begin{pmatrix} p'_k \\ q'_k \end{pmatrix}$$

□

定理 5. 次の条件は同値である:

1. 次の (x, y) は $Ax^2 + Bxy + Cy^2 = N$ の整数解である:

$$x = c_{n+1}p'_n + c_{n+2}p'_{n+1} + \cdots + c_{n+m}p'_{n+m-1},$$
$$y = c_{n+1}q'_n + c_{n+2}q'_{n+1} + \cdots + c_{n+m}q'_{n+m-1}.$$

2. 次の (x, y) は $Ax^2 + Bxy + Cy^2 = (-1)^l N$ の整数解である:

$$x = c_{n+1}p'_{n+l} + c_{n+2}p'_{n+1+l} + \cdots + c_{n+m}p'_{n+m-1+l},$$
$$y = c_{n+1}q'_{n+l} + c_{n+2}q'_{n+1+l} + \cdots + c_{n+m}q'_{n+m-1+l}.$$

□

定理 6. (x, y) は $Ax^2 + Bxy + Cy^2 = N$ (ただし $A > 0$) の整数解であるとする. ここで, $(x - \alpha y)N > 0$ としてよい. さもなくば, $(-x, -y)$ を改めて (x, y) にとる. このとき, x, y は次の形で一意的に表される:

$$x = c_{n+1}p'_n + c_{n+2}p'_{n+1} + \cdots + c_{n+m}p'_{n+m-1},$$
$$y = c_{n+1}q'_n + c_{n+2}q'_{n+1} + \cdots + c_{n+m}q'_{n+m-1}.$$

ただし, $\{c_k\}$ は次を満たすものとする:

1. $c_{n+1} \neq 0$, $c_{n+m} \neq 0$;
2. $0 \leq c_{n+k} \leq a'_{n+k}$;

3. $c_{n+k} = a'_{n+k}$ ならば $c_{n+k-1} = 0$.

さらに, 線型和の長さ m の範囲は A, B, C と N により明示的に評価できる ([3] を参照されたい). □

定理 6 における解の表現の一意性が整数の Ostrowski 表現の一意性から導かれることは, 定理 4 と同様である. そこで, 以下ではこの定理における整数解の表現を, 不定方程式 $Ax^2 + Bxy + Cy^2 = N$ に関する Ostrowski 表現と呼ぶことにする.

例 7. $11x^2 - 24xy + 10y^2 = 45$ の整数解について考える.

$$\alpha = \frac{12 + \sqrt{34}}{11} = [1, 1, \overline{1, 1, 1, 1, 3, 3}]$$

k	-3	-2	-1	0	1	2	3	4	5	6	7	8	9
a_k				1	1	1	1	1	1	3	3	1	1
p_k			1	1	2	3	5	8	13	47	154	201	355
q_k			0	1	1	2	3	5	8	29	95	124	219
a'_k	1	1	1	3	3	1	1	1	1	3	3	1	1
p'_k	-5	4	-1	1	2	3	5	8	13	47	154	201	355
q'_k	-9	7	-2	1	1	2	3	5	8	29	95	124	219

補題 3 に対応することとして, 次の等式が成り立つ:

$$\begin{pmatrix} p'_{k+6} \\ q'_{k+6} \end{pmatrix} = \begin{pmatrix} 107 & -60 \\ 66 & -37 \end{pmatrix} \begin{pmatrix} p'_k \\ q'_k \end{pmatrix}.$$

つまり, 行列 $\begin{pmatrix} 107 & -60 \\ 66 & -37 \end{pmatrix}$ をかけることと添字を $l = 6$ だけずらすこととが対応している.

さて, $(1, -1)$ は $11x^2 - 24xy + 10y^2 = 45$ の整数解であることは容易にわかる. この解の Ostrowski 表現を求めてみよう.

$$\begin{pmatrix} 107 & -60 \\ 66 & -37 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \end{pmatrix} = \begin{pmatrix} 167 \\ 103 \end{pmatrix}$$

より, 別の整数解として $(167, 103)$ がみつかる. 103 の α に関する Ostrowski 表現は $103 = q'_5 + q'_7$ であり, $167 = p'_5 + p'_7$ も成り立つ. 添

字を 6 減らすことで,

$$1 = p'_{-1} + p'_1, \quad -1 = q'_{-1} + q'_1$$

がわかる. □

REFERENCES

[1] 橋本 竜太. 整数の Ostrowski 表現と 2 元 2 次不定方程式の求解について. 第 3 回「代数学と計算」(AC99) における講演. 1999.
to appear in ftp://tnt.math.metro-u.ac.jp/pub/ac99/

[2] Hashimoto, Ryūta. Note on a theorem of Rockett and Szüsz on a diophantine equation $x^2 - Dy^2 = N$. *submitted.*

[3] Hashimoto, Ryūta. (仮題) On a form of the integer solutions of a binary quadratic diophantine equation. *in preparation.*

[4] Rockett, Andrew M. and Szüsz, Peter. A localization theorem in the theory of diophantine approximation and an application to Pell's equation, *Acta Arith.*, 47(4):347–350, 1986.

[5] Rockett, Andrew M. and Szüsz, Peter. *Continued Fractions.* World Scientific, Singapore, 1992.

E-mail address: ryuuta@math.human.nagoya-u.ac.jp
URL: http://www.math.human.nagoya-u.ac.jp/~ryuuta/